UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,193	04/21/2005	Alain Durand	PF030167	8417

24498 7590 11/14/2008

Joseph J. Laks
Thomson Licensing LLC
2 Independence Way, Patent Operations
PO Box 5312
PRINCETON, NJ 08543

EXAMINER	
SHEPELEV, KONSTANTIN	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,193	DURAND ET AL.	
	Examiner	Art Unit	
	KONSTANTIN SHEPELEV	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Applicant's communication filed on August 7, 2008 in response to PTO Office Action mailed May 14, 2008. The Applicant's remarks and amendments to the claims and/or the specification were considered with the results that follow.

Specification Amendments

1. Examiner acknowledges receiving amendments to the specification, which were received by the Office on August 7, 2008. The amendments to the specification included correction of paragraph [0067]. The specification has been updated accordingly to reflect the amendment. The initial objection to the specification has been withdrawn in view of received amendment.

Response to Arguments

2. Applicant's arguments, filed August 7, 2008, with respect to the rejections of claims 1-4 under Diehl et al. (US 2003/0108206 A1) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, new grounds of rejection are made in view of Allan et al. (US 5,870,475).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Allan et al. (US 5,870,475) in view of Menezes et al. "Handbook of Applied Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FI, CRC Press, US, 1997, pages 497-553.

With respect to claim 1, Allan teaches the limitations of "a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network" and "said first symmetric key encrypted with a second symmetric network key known only by at least one device of a second type connected to said network" (Abstract; column 3, lines 37-40) as the working keys of this symmetric key encryption scheme are provided in the head end and the end station, where (column 3, lines 44-46) the end station represents a relatively secure end station, which includes its own public and private keys of a PPK encryption scheme, (column 3, lines 61-62) the head end also has its own public and private keys of a PPK encryption scheme, and (column 4, lines 58-63) the head end randomly generates a working key for communicating signal in a symmetric key encryption scheme, and encrypts this working key in accordance with the supplied public key of the end station, sending the encrypted working key in a message to the end station.

In addition, Allan teaches the limitation of "encrypting the data to be transmitted with the new symmetric key" (column 3, lines 30-34) as for secure and/or private communication of the signals, the head end includes an encryption engine which encrypts the signals in accordance with a working key known only by the head end and the intended end station.

Finally, Allan teaches the limitation of "transmitting to a device of a second type, via said network, the data encrypted with the new symmetric key, the random number, and said first

symmetric key encrypted with the second symmetric network key" (column 5, lines 2-8) as the head end and the end station then load their encryption engines with the working key, and thereafter communications between them take place with data encrypted in accordance with the working key.

It is noted, however, that Allan does not explicitly teach the limitations of "generating a random number" and "computing a new symmetric key as a function of the first symmetric key and said random number."

On the other hand, Menezes discloses abovementioned limitations (pages 552-553, Example 13.9) as C decrypts the key list to obtain Kx, computes S from R, then encrypts S under Kx and transmits it to X. S is analogously transmitted to Y, and can be recovered by both X and Y. Where, C is a Central trusted node, X and Y are terminals, Kx is a terminal key for the terminal X, S is a session key, and R is a random value.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate teachings of Menezes into the system of Diehl because it would increase the security for the transmitted data through the use of the key-encrypting key.

With respect to claim 2, Menezes teaches the limitation of "the function used to compute the new symmetric key is a one-way derivation function" (page 498, lines 5-6) as choosing to be a one-way function precludes control of the final key value by either party.

With respect to claim 4, Allan teaches the limitation of "decrypting, with the second symmetric network key, the encryption of the first symmetric key" (column 4, lines 64-65) as the

end station decrypts the encrypted working key from this message in accordance with its private key.

In addition, Allan teaches the limitation of "decrypting the data received with the new symmetric key thus obtained" (column 5, lines 2-8) as the head end and the end station then load their encryption engines with the working key, and thereafter communications between them take place with data encrypted in accordance with the working key.

It is noted, however, that Allan does not teach the limitation of "determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key."

On the other hand, Menezes teaches (page 553, lines 1-2) the session key derived as a function of a random number and master key.

It would be obvious to one of the ordinary skill in the art that random value R can be obtained from the session key through the application of the function to the master key.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Allan et al. (US 5,870,475) in view of Menezes et al. "Handbook of Applied Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FI, CRC Press, US, 1997, pages 497-553 as applied to claim 1 above, and further in view of Fischer (US 5,475,826).

With respect to claim 3, it is noted that neither Allan nor Menezes disclose the limitation of "the function is a hash or encryption function."

On the other hand, Fischer discloses the abovementioned limitation (column 1, lines 37-39) as It is well-known that file integrity may be protected by taking a one-way hash (e.g., by using MD5 or the secure hash algorithm SHA).

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Fischer into the system of Fischer and Menezes because the use of one-way has would facilitate better protection of the encryption key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 8:30 - 18:00, Fri 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/ 11/07/200
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431